

Evaluation Scoring

Remember to be consistent with scoring methodology

0	Did not provide an answer
2	Incoherent, communicates a lack of understanding and/or capability
4	Marginal, communicates a weak knowledge, understanding, and/or capability
6	Average, communicates an average knowledge, understanding, and/or capability
8	Good, communicates that they are good at what they do and have a good understanding
10	Excellent, communicates that they are not just good, but provide value added services and capabilities that may exceed expectations

Give one score for each question - the average of all scores will be the total points awarded for the interview.

Vendor: Emagined							
Interview Total 10 pts							
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 5	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Average Score							
Average per Evaluator							
Clark	9.71						
Fox	10						
Hjermstad	8.29						
Johnson	9.57						
Laska	9.71						
Toth	8.29						
Total Average for group	9.26						
Notes from Group	Professional, thorough and detailed responses. Gave great examples with specifics.						

Vendor: KPMG							
Interview Total 10 pts							
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 5	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Average Score							
Average per Evaluator							
Clark	6.86						
Fox	8.57						
Hjermstad	5.71						
Johnson	7.71						
Laska	8.57						
Toth	7.71						
Total Average for group	7.52						
Notes from Group	Spoke more about methodology and not very specific in answering questions - felt that it was more from a auditor perspective (over the shoulder review) instead of from a pen testers perspective particulary with Mainframe testing. Limited experience with SCADA/Mainframe systems. Did not show as much depth of knowledge with responses to questions. Impressed with ability to scale up or down.						

Vendor: Online							
Interview Total 10 pts							
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 5	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Average Score							
Average per Evaluator							
Clark	7.71						
Fox	8.29						
Hjermstad	6						
Johnson	7.14						
Laska	9.43						
Toth	9.43						
Total Average for group	8						
Notes from Group	Spoke more about methodology and not very specific in answering questions unless prompted. Limited experience with SCADA. Good explanation on communication.						

Vendor: SAC							
Interview Total 10 pts							
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 5	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Average Score							
Average per Evaluator							
Clark	4.57						
Fox	6						
Hjermstad	5.71						
Johnson	7.86						
Laska	8.86						
Toth	8.57						
Total Average for group	6.93						
Notes from Group	Installing of an SIEM to monitor endpoints during testing is a concern as it would require extensive pre-approval and could cause delays or work stoppage. During discussion it was mentioned that it was intentional and normal to DOS, tip over servers this would cause issues with our auditees. Team seemed to be less cohesive with some answers.						

Vendor: Soteria							
Interview Total 10 pts							
Question 1	Many of the state agencies and local governments we work with have thick client applications that we test. Can you describe your experience with penetration testing thick client applications?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 2	Our engagements can include testing of SCADA systems. In some cases this testing must be done in production on critical systems such as water or sewer treatment plants. Can you describe your penetration testing experience with SCADA systems? What are some of the key questions you would have for the client to ensure a smooth valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 3	Our engagements sometimes include testing mainframes. These would typically be legacy applications that support core or enterprise functions, and therefore may not be as stable or robust as more modern applications. Can you describe your experience with penetration testing mainframes? What are some of the key pieces of information you would want from the client to ensure a smooth and valuable test of a mainframe?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 4	Our engagements sometimes include mobile applications? Can you describe your experience with penetration testing mobile systems? What are some of the key questions you would have for the client to ensure a smooth and valuable test?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 5	Can you describe a time when something went wrong during a prior penetration testing engagement? How did you find out something went wrong? How did you respond or correct the situation? What lessons were learned from that event?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 6	From time to time we need to have more than one penetration testing engagement going simultaneously- with each engagement likely having internal and external testing with approximately 4-6 applications and network testing. Would your firm be able to staff this? If so, how much lead time would your firm require? How many penetration staff would you be able to commit to each engagement? How long would it take your staff to complete a typical penetration test of this size?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Question 7	Communication is an important part of penetration testing work, especially because the systems we test are not managed by SAO, but rather our auditees. Can you tell us about any experience you have testing a third-party application, for example a vendor for your direct client? What type of communication challenges did you face? How did you overcome those challenges?						
Score	0-no answer	2-lack of understanding	4-Marginal	6-Average	8-Good	10-Excellent	Evaluator Score
Average Score							
Average per Evaluator							
Clark	7.43						
Fox	9.71						
Hjermstad	6.57						
Johnson	9						
Laska	9.43						
Toth	9.14						
Total Average for group	8.55						
Notes from Group	Some evaluators thought response to Mobile applications was not as thorough as other questions. Capacity concerns with response on testing windows being longer.						